Department of CEE/ Computer Science

Social Engineering: Hacking the Human Element

Mason Pawsey, Sonia Patino, Marissa Campos, Stephanie Acosta

Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

Research Experience Vitalizing Science — University Program

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service: Scholarship for Service (SFS) program under Award No. 1241636.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Introduction

Today's companies must perform transactions and processes that involve handling data. That data can be company information, personal data, logistic information, etc. This information, if sold to the right person, can yield a massive profit for malicious agents. This provides motive for hackers to target the company. Hacking is the breaching of security to obtain information or some sort of good for personal gain. Companies are very aware of the problem that hacking poses, however, they often overlook a more simple approach for the hacker to compromise a company, social engineering.

What is social engineering?

Social engineering is a tool widely used and often overlooked by companies. It exploits the weakest link in any security protocol, the human element. By preying on human nature, human tendencies, etc, hackers get useful personal/professional information that's then used to breach security.

Purpose

On a daily basis, thousands of attacks are launched against large and small companies to gather private and useful information of consumers around the world.

Our purpose is to explore the methods of attackers, to help protect private information and educate consumers like you and I.

Techniques

- Information Gathering
- Communication Modeling
- Pre-texting
- Elicitation

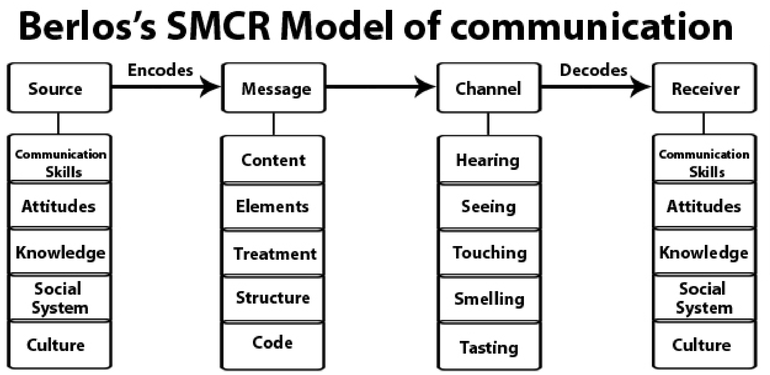
"Know thyself, know thy enemy. A thousand battles, a thousand victories."
– Sun Tzu

Information Gathering

Gathering information about your target is the most integral part of social engineering. Private Information, public information, any kind of information is gathered to create a foundation for the social engineering engagement.

Communication Modeling

The way a social engineer communicates is vital to their information gathering. Gaining someone's trust depends on both their verbal and non verbal means, such as speech, tone of voice, body language, and touch. Because of the human nature, approaching someone in the right way will usually result in a polite and friendly encounter.



Pre-texting

Pre-texting is a false motive that involves creating a new identity. Just like information gathering and communication modeling, pre-texting is a technique used by social engineers to persuade their target to release information or perform some action.

For example, a social engineer could pretend to be an employee of a big company and use the information gathering technique to compromise their security and possibly have physical access to their computers and networks

Elicitation

This is a non-threatening, easy to disguise and effective technique that can be conducted in person, over the phone, or in writing. Elicitors may collect information about you or colleagues that could facilitate future targeting attempts. A trained elicitor exploits certain human or cultural predispositions. This includes: a tendency to answer truthfully when asked an "honest" question, a desire to be polite and helpful, a tendency to gossip, and a tendency to correct others.

PREVENTION

Information Gathering

It would be in the company's best interest to train their employees and inform them of the techniques social engineers use.

Documents that contain personal information and company information should be disposed in a safe way, such as shredding and using secure disposal personnel to keep the information away from dumpster divers.

Communication Modeling/Pre-texting/Elicitation

Just because someone approaches you in a friendly way or looks the part does not mean that they are trustworthy. While it is not necessary to be cold and hostile towards to those who try to strike up conversation, it's important to guard against possible infiltrations. You should not access your personal email through a company's network, and company information should be discussed with authorized personnel only.

It is best to know what information is NOT safe to give. Companies should inform their personnel of what information is acceptable to divulge.

91% of all passwords are one of the 1,000 most common

Conclusion

Companies spend outrageous amounts of money a year ensuring their security systems stay secure to protect their vendors and customers. Unfortunately, they often overlook the most important - and least secure - component of any system: the human element. Social engieering aims to exploit the lack of focus and diligence of employees with critical information that could lead to a breach in security. During our research, we explored the techniques and strategies used to compromise systems and what corporations can do to make sure their people and their sensitive data stays safe and secure.

How many of your passwords are based around YOUR personal information? **Tip**: Use upper/lower case letters, numbers and symbols to eliminate the chances of your password being guessed.

Acknowledgements

•Chevron

•National Science Foundation

•Cal State University of Bakersfield

Works Cited

Burnett, Mark. "10,000 Top Passwords." *Xato Passwords Security 10000 Top Passwords Comments*. Xato, 20 June 2011. Web. 04 Aug. 2014.

Hadnagy, Christopher. *Social Engineering: The Art of Human Hacking*. Indianapolis, IN: Wiley, 2011. Print. .